Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (currently amended) A method of thwarting denial of service attacks on a victim data center coupled to a network, the method comprising ~~comprises~~:

monitoring network traffic through monitors disposed at a plurality of points in the network; ~~and~~

communicating data from the monitors to a central controller, over a redundant network[[,]] that is a different network from the network being monitored;

analyzing the data comprising network traffic statistics to identify network traffic that is part of a denial of service attack; and

filtering the network traffic based on results of analyzing the network traffic to discard network traffic that is identified as part of the denial of service attack~~, to a central controller~~.

2. (currently amended) The method of claim 1, further comprising:

arranging the monitors and central controller to be coupled to the ~~hardened~~ redundant network that is inaccessible to the denial of service attack.

3. (currently amended) The method of claim 1 further comprising:

monitoring network traffic at an edge of the network to protect the data center, with monitoring using a gateway that passes network packets, the gateway disposed at the edge of the network, and with the gateway coupled to the control center by the redundant ~~hardened~~ network.

4. (Original) The method of claim 1 further comprising:

~~analyzing network traffic statistics to identify malicious network traffic; and~~

~~filtering the network traffic based on results of analyzing the network traffic to discard network traffic that is identified as malicious network traffic during analyzing of the network traffic.~~

5. (Previously Presented) The method of claim 3 wherein monitoring network traffic through the gateway occurs at network entry points of victim data centers.

6. (Currently Amended) The method of claim 1 wherein analyzing further ~~comprising~~ comprises:

performing intelligent traffic analysis based on collected statistical data from the monitors ~~and filtering to identify the malicious traffic~~ and filtering further comprises filtering the traffic according to the traffic analysis to eliminate the ~~malicious~~ traffic identified as part of the denial of service attack.

7. (Currently Amended) The method of claim ~~3~~ 6 wherein performing intelligent traffic analysis and filtering, further comprises performing intelligent traffic analysis and filtering by the gateways and the control center.

8. (Currently Amended) The method of claim ~~3~~ 6 wherein performing intelligent traffic analysis and filtering, further comprises performing intelligent traffic analysis and filtering by the gateways.

9. (Currently Amended) The method of claim 1 wherein monitoring network traffic further comprises monitoring network traffic by data collectors sampling packet traffic and accumulating and collecting statistical information about network flows and the method further comprises:

aggregating packet traffic and accumulated statistical information in the control center to coordinate measures to track down and block the sources of an attack.

10. (Previously Presented) The method of claim 9 wherein monitoring network traffic further comprises monitoring network traffic at major peering points and network points of presence.

11. (Previously Presented) The method of claim 1 further comprising:

aggregating traffic information in the control center to coordinate measures to track down and block the sources of an attack.

12. (Original) A distributed system to thwarting denial of service attacks comprises:

a plurality of monitors dispersed throughout a network, the monitors collecting statistical data for performance of intelligent traffic analysis and filtering to identify malicious traffic and to eliminate the malicious traffic to thwart the denial of service attack.

13. (Original) The distributed system of claim 12 further comprising:

a control center coupled to the plurality of data collectors by a hardened redundant connection to communicate the data to the control center; and wherein the control centers performs the intelligent traffic analysis to identify the malicious traffic.

14. (Original) The distributed system of claim 13 further comprising:

at least one gateway device that passes network packets between the network and the victim site, the gateway disposed to protect a victim site, and being coupled to the control center by the redundant hardened network.

15. (Currently Amended) A system for thwarting denial of service attacks on a victim data center coupled to a network comprises:

a first plurality of monitors that monitor network traffic flow through the network, the first plurality of monitors disposed at a second plurality of points in the network; and

a central controller that receives data from the plurality of monitors, over a different redundant network, the central controller analyzing network traffic statistics to identify malicious

network traffic and to coordinate the first plurality of monitors to filter the network traffic based on results of analyzing the network traffic to discard network traffic that is identified as malicious traffic.

16. (Previously Presented) The system of claim 15 wherein the different, redundant network is inaccessible to the attack.

17. (Previously Presented) The system of claim 15 further comprising:

at least one gateway that passes network packets between the network and the victim data center, the gateway disposed to protect potential victim data center and being coupled to the control center by the different, redundant network.

18. (Original) The system of claim 17 wherein the gateway is disposed at an edge of the network at victim data center.

19. (Original) The system of claim 17 wherein the gateway analyzes network traffic statistics to identify malicious network traffic and filters the network traffic based on results of analyzing the network traffic to discard network traffic that is identified as malicious network traffic during analyzing of the network traffic.

20. (Original) The system of claim 17 wherein the gateway is located at the edge of the network that is an entry point to the victim data center.

21. (Original) The system of claim 17 wherein both the gateway and the control center perform intelligent traffic analysis and filtering to identify the malicious traffic and to eliminate the malicious traffic.

22. (Original) The system of claim 15 wherein the data collectors sample packet traffic, and accumulate and collect statistical information about network flows.

23. (Original) The system of claim 15 wherein the data collectors are located at major peering points and network points of presence.

24. (Original) The system of claim 17 wherein the data collectors sample packet traffic, and accumulate and collect statistical information about network flows and are located at major peering points and network points of presence.

25. (Original) The system of claim 17 wherein the control center aggregates traffic information and coordinates measures to track down and block the sources of an attack.

26. (Previously Presented) The system of claim 17 wherein the gateway includes a process to communicate with the control center over the different, redundant network.

27. (Original) The system of claim 17 wherein the gateway includes a process to allow an administrator to insert filters to discard packets that are deemed to be part of an attack, as determined by heuristics of the traffic flow.

28. (Previously Presented) A distributed system to thwart denial of service attacks comprises:

a plurality of gateways dispersed throughout a network, near data centers that might be sources of an attack, the gateways collecting statistical data for performance of intelligent traffic analysis and filtering, identify malicious traffic at the source of an attack, to eliminate the malicious traffic and thwart the denial of service attack.

29. (Previously Presented) The distributed system of claim 28 further comprising:

a control center coupled to the plurality of gateways by a different, redundant network to communicate the data from the gateways to the control center, with the control center performing the intelligent traffic analysis to identify the malicious traffic.

30. (Previously Presented) The distributed system of claim 28 further comprising:

a first plurality of monitors that monitor network traffic flow through the network, the first plurality of monitors disposed at a second plurality of points in the network; and

a central controller that receives data from the plurality of monitors, over a redundant network that is a different network from the network monitored by the monitors, the central controller analyzing network traffic statistics to identify malicious network traffic.

31. (Previously Presented) The distributed system of claim 28 wherein the gateways are disposed at an edge of the network at the victim data centers.

32. (Previously Presented) The system of claim 28 wherein the gateways analyze network traffic statistics to identify malicious network traffic and filter the network traffic based on results of analyzing the network traffic to discard network traffic that is identified as malicious network traffic during analyzing of the network traffic.

33. (Previously Presented) The system of claim 28 wherein the gateway is located at the edge of the network that is an entry point to the victim data center.

34. (Previously Presented) The system of claim 29 wherein both the gateways and the control center perform intelligent traffic analysis and filtering to identify the malicious traffic and to eliminate the malicious traffic.

35. (Previously Presented ) The system of claim 29 wherein the gateways include a process to communicate with the control center over the different, redundant network.

36. (Previously Presented) The system of claim 28 wherein the gateways include a process to allow an administrator to insert filters to discard packets that are deemed to be part of an attack, as determined by heuristics of the traffic flow.